

16.12.2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2004年 1月 8日
Date of Application:

出願番号 特願2004-003431
Application Number:
[ST. 10/C]: [JP 2004-003431]

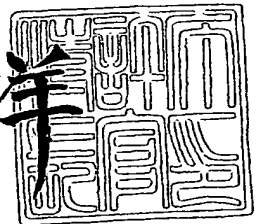
出願人 松下電器産業株式会社
Applicant(s):

BEST AVAILABLE COPY

2005年 1月28日

特許庁長官
Commissioner,
Japan Patent Office

小川 洋



出証番号 出証特2005-3004024

【書類名】 特許願
【整理番号】 2048160002
【あて先】 特許庁長官殿
【国際特許分類】 G09C 1/00 640
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 庭野 智
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 岡本 隆一
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 徳田 克己
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 村上 弘規
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100109210
 【弁理士】
 【氏名又は名称】 新居 広守
【手数料の表示】
 【予納台帳番号】 049515
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 0213583

【書類名】特許請求の範囲**【請求項1】**

暗号化コンテンツを配信するコンテンツ配信サーバと、少なくとも前記暗号化コンテンツを復号するコンテンツ鍵と、前記暗号化コンテンツの利用条件と、デジタル署名を含む端末装置での処理に用いる少なくとも1種類のフォーマットのライセンスを生成し、配信するライセンス管理サーバと、前記ライセンス管理サーバが配信する前記ライセンスとその内容が同一でフォーマットが異なる伝送用のライセンスを前記端末装置に配信するライセンス中継サーバと、前記暗号化コンテンツと前記処理に用いるフォーマットのライセンスと、前記伝送用のフォーマットのライセンスを受信する前記端末装置から構成されるコンテンツ配信システムにおいて、

前記端末装置が前記ライセンス中継サーバから受信した前記伝送用のフォーマットのライセンスを前記ライセンス管理サーバから受信する前記処理に用いるフォーマットのライセンスに変換する少なくとも1つのフォーマット変換手段を有すること特徴とするコンテンツ配信システム。

【請求項2】

前記ライセンス管理サーバが、ライセンス中継サーバに、前記処理に用いるフォーマットを特定する変換フォーマット指定情報を配信することを特徴とする請求項1に記載のコンテンツ配信システム。

【請求項3】

前記ライセンス中継サーバが、前記伝送用のライセンスに前記処理に用いるフォーマットを特定する変換フォーマット指定情報を格納することを特徴とする請求項1に記載のコンテンツ配信システム。

【請求項4】

前記端末装置の前記フォーマット変換手段が、前記ライセンス中継サーバから受信した前記伝送用のライセンスに格納された前記処理に用いるフォーマットを特定する変換フォーマット指定情報に基づき前記伝送用のライセンスを前記処理に用いるフォーマットのライセンスに変換すること特徴とする請求項3に記載のコンテンツ配信システム。

【請求項5】

前記ライセンス管理サーバが、ライセンス中継サーバに、前記処理に用いるフォーマットにおけるデジタル署名を配信することを特徴とする請求項1に記載のコンテンツ配信システム。

【請求項6】

前記ライセンス中継サーバが、前記伝送用のライセンスに前記処理に用いるフォーマットにおけるデジタル署名を格納することを特徴とする請求項1に記載のコンテンツ配信システム。

【請求項7】

前記フォーマット変換手段が前記伝送用のライセンスからフォーマット変換した前記処理に用いるライセンスを、前記処理に用いるフォーマットにおけるデジタル署名を用いて署名検証するライセンス判定手段を有すること特徴とする請求項6に記載のコンテンツ配信システム。

【請求項8】

前記ライセンス管理サーバが前記端末装置での処理に用いるフォーマットのライセンス生成する時に前記ライセンスを特定するライセンスIDを生成し、前記端末装置が前記伝送用のフォーマットのライセンスからフォーマット変換した後に前記ライセンスIDを復元し、前記ライセンスIDでライセンスを管理することを特徴とする請求項1に記載のコンテンツ配信システム。

【請求項9】

暗号化コンテンツを配信するコンテンツ配信サーバと、少なくとも前記暗号化コンテンツを復号するコンテンツ鍵と、前記暗号化コンテンツの利用条件と、デジタル署名を含む端末装置での処理に用いる少なくとも1種類のフォーマットのライセンスを生成し、配信

するライセンス管理サーバと、前記ライセンス管理サーバが配信する前記ライセンスとその内容が同一でフォーマットが異なる伝送用のライセンスを前記端末装置に配信するライセンス中継サーバと、前記暗号化コンテンツと前記処理に用いるフォーマットのライセンスと、前記伝送用のフォーマットのライセンスを受信する前記端末装置から構成されるコンテンツ配信システムにおいて、

前記端末装置が前記ライセンス中継サーバから受信した前記伝送用のフォーマットのライセンスを前記ライセンス管理サーバから受信する前記処理に用いるフォーマットのライセンスに変換するフォーマット変換すること特徴とするライセンス配信方法。

【請求項10】

前記ライセンス管理サーバが、ライセンス中継サーバに、前記処理に用いるフォーマットを特定する変換フォーマット指定情報を配信し、前記ライセンス中継サーバが、前記伝送用のフォーマットのライセンスに前記処理に用いるフォーマットを特定する変換フォーマット指定情報を格納し、前記端末装置の前記フォーマット変換手段が、前記変換フォーマット指定情報に基づき前記伝送用のフォーマットのライセンスを前記処理に用いるフォーマットのライセンスに変換することを特徴とする請求項9に記載のライセンス配信方法。

【請求項11】

前記ライセンス管理サーバが、ライセンス中継サーバに、前記処理に用いるフォーマットにおけるデジタル署名を配信し、前記ライセンス中継サーバが、前記伝送用のライセンスに前記処理に用いるフォーマットにおけるデジタル署名を格納し、前記端末装置の前記フォーマット変換手段が、前記ライセンス中継サーバから受信した前記伝送用のライセンスに格納された前記処理に用いるフォーマットにおけるデジタル署名を用いて、前記伝送用のライセンスからフォーマット変換した前記処理に用いるライセンスを署名検証すること特徴とする請求項9に記載のライセンス配信方法。

【請求項12】

前記ライセンス管理サーバが前記端末装置での処理に用いるフォーマットのライセンス生成する時に前記ライセンスを特定するライセンスIDを生成し、前記端末装置が前記伝送用のフォーマットのライセンスからフォーマット変換した後に前記ライセンスIDを復元し、前記ライセンスIDでライセンスを管理することを特徴とする請求項9に記載のライセンス配信方法。

【請求項13】

暗号化コンテンツを配信するコンテンツ配信サーバと、少なくとも前記暗号化コンテンツを復号するコンテンツ鍵と、前記暗号化コンテンツの利用条件と、デジタル署名を含む少なくとも1種類のフォーマットのライセンスを生成し、配信端末装置での処理に用いる少なくとも1種類のフォーマットのライセンスを生成し、配信するライセンス管理サーバと、前記ライセンス管理サーバが配信する前記ライセンスとその内容が同一でフォーマットが異なる伝送用のライセンスを前記端末装置に配信するライセンス中継サーバと、前記暗号化コンテンツと前記処理に用いるフォーマットのライセンスと、前記伝送用のフォーマットのライセンスを受信する前記端末装置から構成されるコンテンツ配信システムにおいて、

前記端末装置が前記ライセンス中継サーバから受信した前記伝送用のフォーマットのライセンスを前記ライセンス管理サーバから受信する前記処理に用いるフォーマットのライセンスに変換する少なくとも1つのフォーマット変換手段を有すること特徴とする端末装置。

【請求項14】

前記ライセンス中継サーバが、前記伝送用のライセンスに前記処理に用いるフォーマットを特定する変換フォーマット指定情報を格納し、前記端末装置の前記フォーマット変換手段が、前記ライセンス中継サーバから受信した前記伝送用のライセンスに格納された前記処理に用いるフォーマットを特定する変換フォーマット指定情報に基づき前記伝送用のライセンスを前記処理に用いるフォーマットのライセンスに変換すること特徴とする請求項13に記載の端末装置。

【請求項 15】

前記フォーマット変換手段が前記伝送用のライセンスからフォーマット変換した前記処理に用いるライセンスを、前記処理に用いるフォーマットにおけるデジタル署名を用いて署名検証するライセンス判定手段を有すること特徴とする請求項 13 に記載の端末装置。

【書類名】明細書

【発明の名称】コンテンツ配信システム、ライセンス配信方法および端末装置

【技術分野】

【0001】

本発明は、放送および通信を用いて、暗号化した映像、音楽などのデジタルコンテンツ（以下コンテンツと記述）と、少なくともコンテンツの利用条件とコンテンツの暗号化に用いたコンテンツ鍵を含むライセンスを配信し、ユーザが端末装置でコンテンツを利用するシステムに関し、特に、受信したライセンスのフォーマットを変換する端末装置を含むシステムに関する。

【背景技術】

【0002】

近年、デジタルネットワークにより、ユーザの端末装置にコンテンツを配信するシステムが提案されている。ここで、端末装置とは、少なくともCPUと、メモリと、端末装置を制御するソフトウェアから構成される機器のことである。このようなコンテンツ配信システムでは、コンテンツはコンテンツ提供者からユーザの端末装置へ暗号化して配信される。ここで、ライセンスとは、少なくともコンテンツの利用条件とコンテンツの暗号化に用いたコンテンツ鍵を含むデータであり、例えば、コンテンツ提供者などがライセンス発行者として生成する。

【0003】

コンテンツの利用条件には、例えば、“3回利用可能”などの、コンテンツの利用に関する条件が記述されている。端末装置には、ライセンスの利用条件からコンテンツの利用可否を判定し、コンテンツ鍵の利用を制御する、ライセンス処理部がある。

このように、ライセンスにより、ライセンス発行者の意図したとおりのコンテンツ利用を実現する方法はDRM (Digital Rights Management) と呼ばれ、複数のDRM方式が提案されている。

【0004】

コンテンツを提供するコンテンツ提供者には、ユーザによるコンテンツ購入機会拡大のため、複数の配信経路で暗号化コンテンツおよびライセンスを配信したいという要求があり、放送および通信で配信する方法が提案されている。

通常、ライセンスのフォーマットと、ライセンスの処理方法は、DRM方式の方式設計者により規定されるが、例えば、放送では総務省によりコンテンツ鍵の伝送方法が一部規定されているように、DRM方式の方式設計者以外の、例えば、配信事業者などによりライセンスの伝送路上でのフォーマット（以下伝送フォーマットと記述）が一部規定されることがあり、1つのDRM方式でも、配信経路に応じてライセンスの伝送フォーマットを変更する場合がある。

【0005】

従来、特許文献1などに開示されているように、端末装置内での利用条件の処理を共通化するために、配信業者毎に利用条件のフォーマットが異なる場合には、受信した利用条件を内容が同一の統一フォーマットに変換している。

【特許文献1】特開2001-202088号公報

【非特許文献1】ウォーウィック・フォード+マイケル・バウム著「デジタル署名と暗号技術」 株式会社ピアソン・エデュケーション 1997年

【発明の開示】

【発明が解決しようとする課題】

【0006】

端末装置が複数の伝送フォーマットのライセンスを受信する場合には、受信した伝送フォーマットのライセンスを共通の処理用のフォーマット（以下処理フォーマットと記述）に変換することで、ライセンス処理を共通化できるため、端末装置内の処理を効率化することができる。

しかし、端末装置で複数のDRM方式でライセンスを処理する場合には、DRM方式毎にセキュリティを確保することが必要なため、それぞれのDRM方式のライセンス処理部で独自にライセンスを処理することから、DRM方式毎に処理フォーマットが異なることがある。また、DRM方式によっては、サービス毎に処理を分けるなどの理由から、1つのDRM方式でも複数の処理フォーマットを規定することもある。

【0007】

従来の方法では、端末装置がライセンスを処理フォーマットに変換する場合に、ライセンス発行者がライセンス毎にライセンス処理フォーマットを指定することができないという課題を有していた。

さらに、ライセンス発行者がライセンス毎に端末装置でのライセンス処理フォーマットを指定することができたとしても、端末装置におけるフォーマット変換で生成されたライセンスの改ざん検出ができないという課題がある。

【0008】

そして、同じライセンス処理部に対して配信経路に応じて異なるフォーマットで配信したライセンスも配信後は統一的に管理したいという課題がある。

本発明は、こうした従来の問題点を解決するものであり、端末装置でライセンスのフォーマット変換を行うコンテンツ配信システムにおいて、ライセンス発行者によるライセンスの変換フォーマットの指定と、フォーマット変換で生成されたライセンスの改ざん検出と、異なるフォーマットで配信されたライセンスの配信後の統一的な管理を可能とするコンテンツ配信システムを提供することを目的とする。

【課題を解決するための手段】**【0009】**

本発明の請求項1記載のコンテンツ配信システムは、暗号化コンテンツを配信するコンテンツ配信サーバと、少なくとも前記暗号化コンテンツを復号するコンテンツ鍵と、前記暗号化コンテンツの利用条件と、デジタル署名を含む端末装置での処理に用いる少なくとも1種類のフォーマットのライセンスを生成し、配信するライセンス管理サーバと、前記ライセンス管理サーバが配信する前記ライセンスとその内容が同一でフォーマットが異なる伝送用のライセンスを前記端末装置に配信するライセンス中継サーバと、前記暗号化コンテンツと前記処理に用いるフォーマットのライセンスと、前記伝送用のフォーマットのライセンスを受信する前記端末装置から構成されるコンテンツ配信システムにおいて、前記端末装置が前記ライセンス中継サーバから受信した前記伝送用のフォーマットのライセンスを前記ライセンス管理サーバから受信する前記処理に用いるフォーマットのライセンスに変換するフォーマット変換手段を有する。

【0010】

本発明の請求項2記載のコンテンツ配信システムは、前記ライセンス管理サーバが、ライセンス中継サーバに、前記処理に用いるフォーマットを特定する変換フォーマット指定情報を配信する。

本発明の請求項3記載のコンテンツ配信システムは、前記ライセンス中継サーバが、前記伝送用のライセンスに前記処理に用いるフォーマットを特定する変換フォーマット指定情報を格納する。

【0011】

本発明の請求項4記載のコンテンツ配信システムは、前記端末装置の前記フォーマット変換手段が、前記ライセンス中継サーバから受信した前記伝送用のライセンスに格納された前記処理に用いるフォーマットを特定する変換フォーマット指定情報に基づき前記伝送用のライセンスを前記処理に用いるフォーマットのライセンスに変換する。

本発明の請求項5記載のコンテンツ配信システムは、前記ライセンス管理サーバが、ライセンス中継サーバに、前記処理に用いるフォーマットにおけるデジタル署名を配信する。

【0012】

本発明の請求項6記載のコンテンツ配信システムは、前記ライセンス中継サーバが、前

記伝送用のライセンスに前記処理に用いるフォーマットにおけるデジタル署名を格納する。

本発明の請求項 7 記載のコンテンツ配信システムは、前記フォーマット変換手段が前記伝送用のライセンスからフォーマット変換した前記処理に用いるライセンスを、前記処理に用いるフォーマットにおけるデジタル署名を用いて署名検証するライセンス判定手段を有する。

【0013】

本発明の請求項 8 記載のコンテンツ配信システムは、前記ライセンス管理サーバが前記端末装置での処理に用いるフォーマットのライセンス生成する時に前記ライセンスを特定するライセンス ID を生成し、前記端末装置が前記伝送用のフォーマットのライセンスからフォーマット変換した後に前記ライセンス ID を復元し、前記ライセンス ID でライセンスを管理する。

【0014】

本発明の請求項 9 記載のライセンス配信方法は、暗号化コンテンツを配信するコンテンツ配信サーバと、少なくとも前記暗号化コンテンツを復号するコンテンツ鍵と、前記暗号化コンテンツの利用条件と、デジタル署名を含む端末装置での処理に用いる少なくとも 1 種類のフォーマットのライセンスを生成し、配信するライセンス管理サーバと、前記ライセンス管理サーバが配信する前記ライセンスとその内容が同一でフォーマットが異なる伝送用のライセンスを前記端末装置に配信するライセンス中継サーバと、前記暗号化コンテンツと前記処理に用いるフォーマットのライセンスと、前記伝送用のフォーマットのライセンスを受信する前記端末装置から構成されるコンテンツ配信システムにおいて、前記端末装置が前記ライセンス中継サーバから受信した前記伝送用のフォーマットのライセンスを前記ライセンス管理サーバから受信する前記処理に用いるフォーマットのライセンスに変換する。

【0015】

本発明の請求項 10 記載のライセンス配信方法は、前記ライセンス管理サーバが、ライセンス中継サーバに、前記処理に用いるフォーマットを特定する変換フォーマット指定情報を配信し、前記ライセンス中継サーバが、前記伝送用のフォーマットのライセンスに前記処理に用いるフォーマットを特定する変換フォーマット指定情報を格納し、前記端末装置の前記フォーマット変換手段が、前記変換フォーマット指定情報に基づき前記伝送用のフォーマットのライセンスを前記処理に用いるフォーマットのライセンスに変換する。

【0016】

本発明の請求項 11 記載のライセンス配信方法は、前記ライセンス管理サーバが、ライセンス中継サーバに、前記処理に用いるフォーマットにおけるデジタル署名を配信し、前記ライセンス中継サーバが、前記伝送用のライセンスに前記処理に用いるフォーマットにおけるデジタル署名を格納し、前記端末装置の前記フォーマット変換手段が、前記ライセンス中継サーバから受信した前記伝送用のライセンスに格納された前記処理に用いるフォーマットにおけるデジタル署名を用いて、前記伝送用のライセンスからフォーマット変換した前記処理に用いるライセンスを署名検証する。

【0017】

本発明の請求項 12 記載のライセンス配信方法は、前記ライセンス管理サーバが前記端末装置での処理に用いるフォーマットのライセンス生成する時に前記ライセンスを特定するライセンス ID を生成し、前記端末装置が前記伝送用のフォーマットのライセンスからフォーマット変換した後に前記ライセンス ID を復元し、前記ライセンス ID でライセンスを管理する。

【0018】

本発明の請求項 13 記載の端末装置は、暗号化コンテンツを配信するコンテンツ配信サーバと、少なくとも前記暗号化コンテンツを復号するコンテンツ鍵と、前記暗号化コンテンツの利用条件と、デジタル署名を含む端末装置での処理に用いる少なくとも 1 種類のフォーマットのライセンスを生成し、配信するライセンス管理サーバと、前記ライセンス管

理サーバが配信する前記ライセンスとその内容が同一でフォーマットが異なる伝送用のライセンスを前記端末装置に配信するライセンス中継サーバと、前記暗号化コンテンツと前記処理に用いるフォーマットのライセンスと、前記伝送用のフォーマットのライセンスを受信する前記端末装置から構成されるコンテンツ配信システムにおいて、前記端末装置が前記ライセンス中継サーバから受信した前記伝送用のフォーマットのライセンスを前記ライセンス管理サーバから受信する前記処理に用いるフォーマットのライセンスに変換する。

【0019】

本発明の請求項14記載の端末装置は、前記ライセンス中継サーバが、前記伝送用のライセンスに前記処理に用いるフォーマットを特定する変換フォーマット指定情報を格納し、前記端末装置の前記フォーマット変換手段が、前記ライセンス中継サーバから受信した前記伝送用のライセンスに格納された前記処理に用いるフォーマットを特定する変換フォーマット指定情報に基づき前記伝送用のライセンスを前記処理に用いるフォーマットのライセンスに変換する。

【0020】

本発明の請求項15記載の端末装置は、前記フォーマット変換手段が前記伝送用のライセンスからフォーマット変換した前記処理に用いるライセンスを、前記処理に用いるフォーマットにおけるデジタル署名を用いて署名検証するライセンス判定手段を有する。

【発明の効果】

【0021】

本発明の変換フォーマット指定情報によれば、端末装置での処理に用いるフォーマットと異なるフォーマットで配信されたライセンスも、端末装置のフォーマット変換手段が、ライセンスに含まれる変換フォーマット指定情報により指定されるフォーマットのライセンスに変換するため、ライセンス発行者による端末装置におけるライセンスの処理フォーマットの指定と、端末装置における受信後のライセンス処理の共通化が可能になる。

【0022】

また、本発明の処理に用いるフォーマットにおけるデジタル署名により、端末装置での処理に用いるフォーマットと異なるフォーマットで配信されたライセンスを処理に用いるフォーマットに変換した後にデジタル署名によるライセンスの改ざん検出が可能となる。さらに、ライセンス発行者が生成したライセンスIDと一致するライセンスIDをフォーマット変換後のライセンスで復元することにより、異なるフォーマットで配信されたライセンスをライセンス発行者が統一的に管理することが可能となる。

【発明を実施するための最良の形態】

【0023】

以下、本発明の実施の形態について、図面を参照しながら説明する。尚、以下の説明に記述されるコンテンツの暗号化方式は、AES (Advanced Encryption Standard) や Triple DES (Data Encryption Standard) 等の共通鍵暗号アルゴリズムが、デジタル署名の方式には、RSAやECDSA (Elliptic Curve Digital Signature Algorithm) 等の公開鍵暗号アルゴリズムが用いられるのが一般的であり、以下に説明する処理は特定の暗号方式に依存しない。また、ハッシュ計算方式は、SHA-1 (Secure Hash Algorithm 1) やMD5等が用いられるのが一般的であり、本実施の形態は特定のハッシュ計算方式に依存しない。

【0024】

また、本実施の形態では、ライセンスを送受信する場合には、セキュリティを確保するため、SSL (Secure Socket Layer) などの安全な認証チャネル (Secure Authenticated Channel、以下、SACと記述) を確立することなどにより、受信側と共有した暗号鍵、または、あらかじめ構成要素間で共有しておいた暗号鍵を用いて少なくともコンテンツ鍵を暗号して通信を行っている。尚、デジタル署名とそれを使った改ざん検出、および、SACについては、非特許文献1など

が詳しい。

【0025】

図1は、本発明の実施の形態に関わるコンテンツ配信システム1の全体の構成を示す図である。図1に示すように、コンテンツ配信システム1は、ライセンス管理サーバ100と、ライセンス中継サーバ110と、端末装置120と、コンテンツ配信サーバ130とを備え、各々が伝送路Nで接続されている。

ライセンス管理サーバ100は、コンテンツ提供者等のライセンス発行者側に設置される装置であって、少なくとも、コンテンツ配信サーバ130からのコンテンツ情報の受信と、ライセンスの作成と、ライセンス中継サーバ110へのライセンスの送信と、端末装置120へのライセンスの配信とを行う。コンテンツ情報とは、少なくとも、コンテンツIDと、コンテンツ鍵を含むデータである。

【0026】

ライセンス中継サーバ110は、配信事業者等に設置される装置であって、少なくとも、ライセンス管理サーバ100からのライセンス生成情報の受信と、ライセンス生成情報からライセンスへの変換と、端末装置120へのライセンスの配信を行う。

端末装置120は、少なくとも、暗号化コンテンツとライセンスの受信と、ライセンスの伝送フォーマットから処理フォーマットへの変換と、暗号化コンテンツの利用を行う。

【0027】

コンテンツ配信サーバ130は、コンテンツ提供者等に設置される装置であって、少なくとも、暗号化コンテンツの生成と、コンテンツ情報のライセンス管理サーバ100への送信と、暗号化コンテンツの端末装置120への送信を行う。

伝送路Nは、インターネット等の通信ネットワークや、デジタル放送、あるいは、これらが複合したネットワークである。

【0028】

尚、コンテンツ配信システム1には、公開鍵証明書、および、共有する暗号鍵などの管理を行う図示しないCA (Certification Authority) サーバ、および、鍵管理サーバなども接続されているが、本実施の形態では、詳しく説明しない。

次に、コンテンツ配信システム1の各構成要素について説明する。

(構成要素1) ライセンス管理サーバ100

図2は、本発明の実施の形態におけるライセンス管理サーバ100の構成を示す図である。

【0029】

図2において、コンテンツ情報受信部210は、コンテンツ配信サーバ130から、コンテンツ情報を受信する。

ライセンス生成部220は、少なくともコンテンツ情報と、ライセンス発行者が設定した利用条件から、端末装置120に配信する処理フォーマットライセンス510と、ライセンス中継サーバ110に送信するライセンス生成情報を生成する。

【0030】

ライセンス送信部230は、ライセンス中継サーバ110にライセンス生成情報を、端末装置120に処理フォーマットライセンス510をそれぞれ送信する。

(構成要素2) ライセンス中継サーバ110

図3は、本発明の実施の形態におけるライセンス中継サーバ110の構成を示す図である。

【0031】

図3において、ライセンス生成情報受信部310は、ライセンス管理サーバ100からライセンス生成情報を受信する。

ライセンス変換部320は、ライセンス管理サーバ100から受信したライセンス生成情報を変換し、伝送フォーマットライセンス710を生成する。

ライセンス送信部330は、伝送フォーマットライセンス710を端末装置120に送信する。

【0032】

尚、本実施の形態では、ライセンス中継サーバ110が伝送フォーマットライセンス710を生成する場合について記述するが、ライセンス管理サーバ100のライセンス生成部220で伝送フォーマットライセンス710を生成する場合には、ライセンス変換部320がライセンス管理サーバ100に含まれ、ライセンス生成情報受信部310で伝送フォーマットライセンス710を受信することになるが、同様な効果が得られる。

【0033】

(構成要素3) 端末装置120

端末装置120は、耐タンパ部410と、図示しないノンセキュア部から構成される。

ノンセキュア部は少なくともユーザインタフェースなどの処理を行う。以上で端末装置120のノンセキュア部について説明した。

【0034】

図4は、本発明の実施の形態における端末装置120の耐タンパ部410の構成を示す図である。

図4において、耐タンパ部410は、第1のライセンス処理部420と、第2のライセンス処理部421と、コンテンツ処理部450から構成されている。

第1のライセンス処理部420は、伝送フォーマットライセンス710の受信と、ライセンスのフォーマット変換を行う伝送フォーマットAライセンス変換部430と、伝送フォーマットBライセンス変換部431と、処理フォーマットライセンス510の受信と、ライセンス判定処理を行う処理フォーマット α ライセンス判定部440と処理フォーマット β ライセンス判定部441から構成されている。

【0035】

ここで、ライセンス判定処理とは、利用条件判定と、少なくともコンテンツ鍵のコンテンツ処理部450への送信を意味する。

尚、耐タンパ部410の端末装置120への実装は、端末装置120から取り外せない状態で実装する場合と、ICカードなどの可搬型モジュールとして実装する場合があるが、本発明は、どちらの実装でも同様な効果が得られる。

【0036】

尚、本実施の形態では、1つの耐タンパ部410に第1のライセンス処理部420と、コンテンツ処理部450が実装されているが、第1のライセンス処理部420と、コンテンツ処理部450の間に送受信されるデータがSACなどにより安全に保護されるならば、異なる耐タンパ部に実装されても同様な効果が得られる。

尚、本実施の形態では、第1のライセンス処理部420が伝送フォーマットAと、伝送フォーマットBと、処理フォーマット α と、処理フォーマット β に対応する場合について記述するため、第1のライセンス処理部420が、伝送フォーマットAライセンス変換部430と、伝送フォーマットBライセンス変換部431と、処理フォーマット α ライセンス判定部440と処理フォーマット β ライセンス判定部441とから構成されているが、ライセンス処理部には、少なくとも1つの伝送フォーマットライセンス変換部と、1つの処理フォーマットライセンス判定部があれば同様な効果が得られる。

【0037】

第2のライセンス処理部421は、第1のライセンス処理部420とは異なるDRM方式のライセンスを処理するが第1のライセンス処理部420と同様な構成であり、本実施の形態では詳しく説明しない。

尚、本実施の形態では、2つのDRM方式に対応した端末装置120について記述するため、耐タンパ部410に第1のライセンス処理部420と第2のライセンス処理部421があるが、少なくとも1つのライセンス処理部があれば同様な効果が得られる。

【0038】

コンテンツ処理部450は、暗号化コンテンツをコンテンツ鍵で復号し、利用条件に基づき利用処理を行う。

尚、本実施の形態では、端末装置 120 にコンテンツ処理部 450 が 1 つの場合について記述するが、DRM 方式毎に異なるコンテンツ処理部 450 がある場合も同様な効果が得られる。

【0039】

(構成要素 4) コンテンツ配信サーバ 130
コンテンツ配信サーバ 130 は、コンテンツ情報と暗号化コンテンツ 810 を生成し、コンテンツ情報をライセンス管理サーバ 100 に、暗号化コンテンツ 810 を端末装置 120 に配信する。

次に、コンテンツ配信システム 1 の各構成要素が保有するデータについて説明する。

【0040】

(データ 1) 処理フォーマットライセンス 510

図 5 は処理フォーマットライセンス 510 の記述例である。

処理フォーマットライセンス 510 は、少なくとも端末装置 120 の耐タンパ部 410 での処理に用いられる。また、処理フォーマットライセンス 510 は、ライセンス本体 511 と、処理フォーマット署名 512 とから構成されている。

【0041】

ライセンス本体 511 には利用条件、および、コンテンツ鍵が記述される。

処理フォーマット署名 512 には、ライセンス本体 511 に対するライセンス発行者のデジタル署名が記述され、ライセンス本体 511 の改ざん検出に用いる。

図 6 は XML 言語によるライセンス本体 511 と処理フォーマット署名 512 の記述例である。

【0042】

尚、本実施の形態では、処理フォーマットライセンス 510 の記述例として XML 言語で記述された例を示すが、少なくとも、利用条件とコンテンツ鍵が記述できれば他の記述形式でもよい。

図 6 において、<right>はコンテンツの再生または他のメディアへの移動などの利用方法を、<contentID>はコンテンツの識別に用いるコンテンツ ID を、<contentKey>は暗号化コンテンツの復号に用いるコンテンツ鍵を、<maxCount>はコンテンツの最大利用回数を、<drmID>は DRM 方式を特定する識別子を、<version>はライセンスフォーマットのバージョンを、<licenseID>はライセンスの識別に用いるライセンス ID を、<endTimePoint>はライセンスの終了時間を、<signature>は処理フォーマット署名 512 を示し、このライセンスが、“0001” という DRM 方式の、Ver1.0 のライセンスフォーマットで記述された、“02” という ID のライセンスであり、“02” という ID のコンテンツを、2003 年 8 月 31 日 12 時 34 分 56 秒まで、最大 9 回利用可能で、このコンテンツ復号に必要なコンテンツ鍵が 0001 であることを示している。

【0043】

尚、タグを追加することで、図 6 に示す以外の情報項目を追加することができる。

(データ 2) 伝送フォーマットライセンス 710

図 7 は、ライセンス中継サーバ 110 が、ライセンス管理サーバ 100 から受信したライセンス生成情報を基に生成する、図 6 の処理フォーマットライセンスの記述例と同一内容の、伝送フォーマットライセンス 710 の記述例である。

【0044】

伝送フォーマットライセンス 710 は、変換フォーマット指定情報 711 と、処理フォーマット署名 712 と、ライセンス本体 750 と、改ざん検出 760 から構成される。

変換フォーマット指定情報 711 は、端末装置 120 の伝送フォーマットライセンス変換部で、伝送フォーマットライセンス 710 の処理フォーマット署名 712 と、ライセンス本体 750 に含まれる情報項目を処理フォーマットに変換する際の変換フォーマットを指定する情報であり、例えば、処理フォーマット α に変換する場合には、処理フォーマット α を特定する識別子 “ α ” が格納される。

【0045】

尚、本実施の形態では、変換フォーマット指定情報711が処理フォーマットを特定する識別子の場合について記述するが、処理フォーマットが1つしかないDRM方式では、変換するか否かの2値を指定するフラグでも同様な効果が得られる。

処理フォーマット署名712は、処理フォーマットライセンス510の処理フォーマット署名512と同じデータである。

【0046】

ライセンス本体750は、ライセンス本体511に相当する内容であり、本実施の形態では、drmID716が<drmID>に、version719が<version>に、licenseID722が<licenseID>に、right725が<right>に、maxCount728が<maxCount>に、contentID731が<contentID>に、contentKey734が<contentKey>に、endTimePoint737が<endTimePoint>に、それぞれ対応する値が格納される。

【0047】

尚、端末装置120でのフォーマット変換後のライセンス本体511が、ライセンス管理サーバ100で生成したライセンス本体511と一致するならば、ライセンス本体750の各値は、ライセンス本体511の対応する値と異なる場合でも同様な効果が得られる。したがって、フォーマット変換の変換規則をライセンス中継サーバ110と端末装置120が共有していれば、例えば、ライセンス本体511のライセンスIDが“02”であり、本実施の形態では説明しないライセンス中継サーバ110の識別番号が“01”であり、ライセンス本体750のライセンスIDが、ライセンス本体511におけるライセンスIDの先頭にライセンス中継サーバ110の識別番号が付加するという変換規則により、“0102”となる場合でも、端末装置120でライセンス本体750からライセンス本体511にフォーマット変換する時に、ライセンス中継サーバ110の識別番号に対応するライセンス本体750のライセンスIDの先頭部分“01”を削除することで、ライセンス本体511のライセンスIDを“02”にすることができれば、同様な効果が得られる。

【0048】

尚、本実施の形態では、ライセンス本体511と、ライセンス本体750の対応する値は一致しているが、以下の説明ではライセンス本体の各値については説明しない。

記述子タグ714には、drmIDを特定する識別子が、記述子長715には、drmID716のバイト長が、記述子タグ717には、versionを特定する識別子が、記述子長718には、version719のバイト長が、記述子タグ720には、ライセンスIDを特定する識別子が、記述子長721には、licenseID722のバイト長が、記述子タグ723には、rightを特定する識別子が、記述子長724には、right725のバイト長が、記述子タグ726には、maxCountを特定する識別子が、記述子長727には、maxCount728のバイト長が、記述子タグ729には、contentIDを特定する識別子が、記述子長730には、contentID731のバイト長が、記述子タグ732には、contentKeyを特定する識別子が、記述子長733には、contentKey734のバイト長が、記述子タグ735には、endTimePointを特定する識別子が、記述子長736には、endTimePoint737のバイト長が、それぞれ格納される。

【0049】

改ざん検出760は変換フォーマット指定情報711から改ざん検出760直前までのバイト列のハッシュ値であり、伝送フォーマットライセンス710の改ざん検出に用いる。

尚、本実施の形態では、改ざん検出710としてハッシュ値を用いるが、デジタル署名など改ざんの検出が可能なデータであれば、同様な効果が得られる。

【0050】

尚、伝送フォーマットライセンス710には、記述子タグを追加することで、図7に示す以外の情報項目を追加することができる。

尚、本実施の形態では、伝送フォーマットライセンス710が記述子形式で記述される場合について説明するが、少なくとも変換フォーマット指定情報711と処理フォーマット署名712が含まれていれば、他の記述形式でも同様な効果が得られる。

【0051】

尚、本実施の形態では、伝送フォーマットAライセンスの例として、伝送フォーマットライセンス710を用いるが、他の伝送フォーマットのライセンスも、少なくとも変換フォーマット指定情報711と処理フォーマット署名712を含む伝送フォーマットライセンス710と類似したデータ構造であれば同様な効果が得られる。

(データ3) 暗号化コンテンツ810

暗号化コンテンツ810は、図8に示す通り、コンテンツID811と、コンテンツ本体812から構成され、コンテンツ本体812はコンテンツ鍵で暗号化されている。

【0052】

コンテンツID811は、ライセンスと暗号化コンテンツ810を対応付けるために用いる。コンテンツ本体812は、映像または音楽などのデジタルデータである。

尚、本実施の形態では、暗号化コンテンツ810にコンテンツID811を含む場合について説明するが、他の方法により暗号化コンテンツ810と処理フォーマットライセンス510が対応付けることができれば、暗号化コンテンツ810にコンテンツID811を含まない構造でも同様な効果が得られる。

【0053】

(データ4) ライセンス生成情報

ライセンス生成情報は、伝送フォーマットライセンス710を生成するために、ライセンス管理サーバ100からライセンス中継サーバ110に送信されるデータで、少なくとも、変換フォーマット指定情報711と、処理フォーマット署名512と、図示しないライセンス本体511と内容同一のデータから構成される。

【0054】

尚、ライセンス生成情報のフォーマットは、ライセンス管理サーバ100とライセンス中継サーバ110との間で規定されていれば、どのようなフォーマットを用いても同様な効果が得られる。

次にコンテンツ配信システム1の構成要素の処理について説明する。
コンテンツ配信システム1におけるライセンスの作成までの処理概略は、例えば、図9に示す手順で行われる。

【0055】

コンテンツ配信サーバ130は、コンテンツと、コンテンツ鍵と、コンテンツID811を生成し、コンテンツをコンテンツ鍵で暗号化してコンテンツ本体812を生成し、コンテンツID811とコンテンツ本体812から暗号化コンテンツ810を生成し、少なくともコンテンツID811とコンテンツ鍵を含むコンテンツ情報をライセンス管理サーバ100に送信(ステップS100)する。

【0056】

尚、本実施の形態では、コンテンツ配信サーバ130からライセンス管理サーバ100にコンテンツ情報としてコンテンツID811を送信する場合について記述するが、ライセンス管理サーバ100がコンテンツID811を生成して、コンテンツ配信サーバ130に送信し、コンテンツ配信サーバ130が暗号化コンテンツとコンテンツID811を関連付けるようにしても同様な効果が得られる。

【0057】

ライセンス管理サーバ100は、コンテンツ情報を受信(ステップS110)し、処理フォーマットライセンス510と、ライセンス中継サーバ110に送信するライセンス生成情報を生成(ステップS120)し、ライセンス生成情報をライセンス中継サーバ110に送信(ステップS130)する。

ライセンス中継サーバ110は、ライセンス生成情報を受信(ステップS140)し、伝送フォーマットライセンス710を生成(ステップS150)する。

【0058】

コンテンツ配信システム1における暗号化コンテンツとライセンスの配信からコンテンツ利用までの処理概略は、例えば、図10に示す手順で行われる。

コンテンツ配信サーバ130は、端末装置120に暗号化コンテンツを配信(ステップS160)する。

端末装置600は、コンテンツ配信サーバ130から暗号化コンテンツを受信(ステップS190)する。

【0059】

ライセンス管理サーバ100は、端末装置120に処理フォーマットライセンス510を配信(ステップS170)する。

端末装置600は、ライセンス管理サーバ100から処理フォーマットライセンス510を受信(ステップS200)し、ライセンスの利用条件などから利用可否を判定(ステップS210)し、端末装置600から受信したコンテンツの利用を制御(ステップS220)する。

【0060】

ライセンス中継サーバ110は、端末装置120に伝送フォーマットライセンス710を配信(ステップS180)する。

端末装置600は、ライセンス中継サーバ110から伝送フォーマットライセンス710を受信(ステップS230)し、処理フォーマットライセンスに変換(ステップS240)し、ライセンスの利用条件などから利用可否を判定(ステップS250)し、端末装置600から受信したコンテンツの利用を制御(ステップS260)する。

【0061】

次に、各構成要素の処理について図面を用いて説明する。

図11を用いて、ライセンス管理サーバ100の処理について説明する。

(コンテンツ情報受信S110)

ライセンス管理サーバ100は、コンテンツ配信サーバ130からコンテンツ情報を受信(ステップS110)する。

【0062】

(ライセンス生成S120)

ライセンス発行者は、ライセンス管理サーバ100に、コンテンツ配信サーバ130から受信したコンテンツ情報に対応する利用条件を入力(ステップS121)する。

ライセンス管理サーバ100は、コンテンツ配信サーバ130から受信したコンテンツ情報と、ライセンス発行者が入力した利用条件から、処理フォーマットでライセンス本体511を生成(ステップS122)し、ライセンス本体511に対する処理フォーマット署名512を生成(ステップS123)する。複数の処理フォーマットを持つDRM方式のライセンス管理サーバ100では、各処理フォーマットに対してステップS122からステップS123の処理フォーマットライセンス510の生成を繰り返す(ステップS124)。

【0063】

尚、本実施の形態では、第1のライセンス処理部420で処理される処理フォーマット α と処理フォーマット β を有するDRM方式について記述するため、ステップS124で2つの処理フォーマットライセンス510を生成するが、少なくとも1つの処理フォーマットライセンス510を生成すれば、同様な効果が得られる。

【0064】

次に、ライセンス管理サーバ100は、ライセンス本体511を送信先のライセンス中継サーバ110とライセンス管理サーバ100との間で規定されているフォーマットに変換し、各処理フォーマットに対応する処理フォーマット署名512と、変換フォーマット指定情報711を付加して、ライセンス生成情報を生成(ステップS125)する。

【0065】

(ライセンス生成情報送信S130)

ライセンス管理サーバ100は、ライセンス中継サーバ110にライセンス生成情報を送信する。

【0066】

(処理フォーマットライセンス送信S170)

次に、ライセンス管理サーバ100は、端末装置120に処理フォーマットライセンス510を送信する。処理フォーマットライセンス510は、送信先の処理フォーマットライセンス判定部に対応したフォーマットであり、本実施の形態では、送信先が、第1のライセンス処理部420の処理フォーマット α ライセンス判定部440の場合について記述するため、処理フォーマット α の処理フォーマットライセンス510である。

【0067】

尚、処理フォーマット α と異なる処理フォーマットライセンス510を送信する場合でも、送信先が処理フォーマット α ライセンス判定部440と異なるが、同様な効果が得られる。

尚、処理フォーマットライセンス510の送信は、端末装置120からの要求に応じてライセンス管理サーバ100が送信する場合と、ライセンス管理サーバ100がブロードキャストした処理フォーマットライセンス510を端末装置120が受信する場合とがあるが、本発明では、特定の送受信方法に依存しないため、どの方法で処理フォーマットライセンス510を送受信しても同様な効果が得られる。

【0068】

尚、端末装置120に複数の処理フォーマットライセンス判定部がある場合でも、それぞれのDRM方式および処理フォーマットで規定された送受信プロトコルにより処理フォーマットライセンス判定部を特定する場合と、処理フォーマットライセンス510に記述した識別子、例えば、本実施の形態の<drmID>および<version>などにより処理フォーマットライセンス判定部を特定する場合とがあるが、本発明では、特定の送受信方法に依存しないため、どの方法で処理フォーマットライセンス判定部を特定しても同様な効果が得られる。

【0069】

図12を用いてライセンス中継サーバ110の処理について説明する。

(ライセンス生成情報受信S140)

ライセンス中継サーバ110は、ライセンス管理サーバ100から、ライセンス生成情報を受信する。

【0070】

(伝送フォーマットライセンス生成S150)

ライセンス中継サーバ110は、ライセンス生成情報から変換フォーマット指定情報711に対応するフォーマットでライセンス本体750を生成し、変換フォーマット指定情報711と、処理フォーマット署名712と、改ざん検出760を付加して、伝送フォーマットライセンス710を生成(S151)する。

【0071】

尚、本実施の形態では、伝送路Nにおける改ざんを検出するために、伝送フォーマットライセンス710にライセンス中継サーバ110が付加した改ざん検出760を含むが、伝送路Nにおける改ざん検出を行わないなど、伝送フォーマットライセンス710の送受信方法によっては伝送フォーマットライセンス710に改ざん検出760がなくても同様な効果が得られる。

【0072】

ライセンス管理サーバ100が複数の処理フォーマットに対応しており、ライセンス中継サーバ110が複数の伝送フォーマットに対応している場合は、ライセンス中継サーバ110は、各処理フォーマットおよび各伝送フォーマットに対して、内容が同一の伝送フォーマットライセンス710の生成を繰り返す(ステップS152)。

(伝送フォーマットライセンス送信S180)
次に、ライセンス中継サーバ110は、端末装置120に伝送フォーマットライセンス710を送信する。伝送フォーマットライセンス710は、送信先の伝送フォーマットライセンス変換部に対応したフォーマットであり、本実施の形態では、送信先が、第1のライセンス処理部420の伝送フォーマットAライセンス変換部430の場合について記述するため、伝送フォーマットAライセンスの伝送フォーマットライセンス710となる。

【0073】

尚、伝送フォーマットAと異なる伝送フォーマットライセンス710を送信する場合でも、送信先が伝送フォーマットAライセンス変換部430と異なるが、同様な効果が得られる。

尚、伝送フォーマットライセンス710の送信は、端末装置120からの要求に応じてライセンス中継サーバ110が送信する場合と、ライセンス中継サーバ110がブロードキャストした伝送フォーマットライセンス710を端末装置120が受信する場合とがあるが、本発明では、特定の送受信方法に依存しないため、どの方法で伝送フォーマットライセンス710を送受信しても同様な効果が得られる。

【0074】

尚、端末装置120に複数の伝送フォーマットライセンス変換部がある場合でも、それぞれのDRM方式および伝送フォーマットで規定された送受信プロトコルにより伝送フォーマットライセンス変換部を特定する場合と、伝送フォーマットライセンス710に記述した識別子、例えば、本実施の形態のdrmID716およびversion719など、により伝送フォーマットライセンス変換部を特定する場合とがあるが、本発明では、特定の送受信方法に依存しないため、どの方法で伝送フォーマットライセンス変換部を特定しても同様な効果が得られる。

【0075】

図13を用いて端末装置120の処理について説明する。

(コンテンツ受信S190)

端末装置120は、コンテンツ配信サーバ130から暗号化コンテンツ810を受信する。

(処理フォーマットライセンス受信S200)

端末装置120の第1のライセンス処理部420の処理フォーマット α ライセンス判定部440は、処理フォーマット α で記述された処理フォーマットライセンス510をライセンス管理サーバ100から受信する。

【0076】

(ライセンス判定S210)

処理フォーマット α ライセンス判定部440は、受信した処理フォーマットライセンス510を、処理フォーマット署名512で検証(ステップS211)する。

尚、本発明は、特定の署名検証方法に依存しないため、少なくとも、署名検証に用いる公開鍵証明書およびCRL(Certificate Revocation List)が取得できれば、どのような署名検証方法を用いても同様な効果が得られる。

【0077】

改ざんが検出されるなど、署名検証に失敗した場合には、コンテンツ利用を中止(ステップS400)する。

改ざんされていないことが確認されると、処理フォーマット α ライセンス判定部440は、処理フォーマットライセンス510から2003年8月31日12時34分56秒までは、処理フォーマットライセンス510から2003年8月31日12時34分56秒まで、最大9回利用可能であることを把握し、例えば、現在時刻が2003年8月1日12時34分56秒で、初回利用であるため、利用可能であると判定(ステップS212)し、コンテンツ処理部450にコンテンツ鍵とコンテンツ処理部でのコンテンツ利用を規定する利用条件を送信する。

【0078】

利用不可と判定した場合は、コンテンツ利用を中止(ステップS400)する。

尚、本発明は、時刻および利用回数などに関して、特定の判定方法に依存しないため、少なくとも不正な判定が防止できれば、どのような判定方法を用いても同様な効果が得られる。

【0079】

(コンテンツ利用S220)

コンテンツ処理部450は、コンテンツ鍵で暗号化コンテンツ810を復号し、利用条件に基づいてコンテンツ利用を制御する。

【0080】

尚、利用条件にコンテンツIDを格納すれば、コンテンツ利用前にライセンスとコンテンツとの対応関係の検証も可能となる。

(伝送フォーマットライセンス受信S230)

端末装置120の第1のライセンス処理部420の伝送フォーマットAライセンス変換部430は、伝送フォーマットAで記述された伝送フォーマットライセンス710をライセンス中継サーバ110から受信する。

【0081】

(変換処理S240)

伝送フォーマットAライセンス変換部430は、受信した伝送フォーマットライセンス710を改ざん検出760で改ざん検出(ステップS241)し、改ざんが検出された場合には、コンテンツ利用を中止(ステップS400)する。

改ざんされていない場合には、伝送フォーマットAライセンス変換部430は、伝送フォーマットライセンス710の変換フォーマット指定情報711に基づき、伝送フォーマットライセンス710を、処理フォーマットライセンス510に変換(ステップS242)する。本実施の形態では、変換フォーマット指定情報711に処理フォーマット α を特定する識別子が含まれており、伝送フォーマットAの伝送フォーマットライセンス710は、処理フォーマット α の処理フォーマットライセンス510に変換される。

【0082】

尚、本発明は、特定のフォーマット変換方法に依存せず、少なくとも、伝送フォーマットライセンス710をフォーマット変換後、ライセンス管理サーバ100で生成した処理フォーマットライセンス510と一致すれば、どのようなフォーマット変換方法を用いても同様な効果が得られる。

尚、本実施の形態では、変換フォーマット指定情報711で伝送フォーマットAライセンス変換部430が変換する処理フォーマットを指定しているが、伝送フォーマットAライセンス変換部430に変換テーブルがあらかじめ設定されている場合には、伝送フォーマットライセンス710に変換フォーマット指定情報711がなくても伝送フォーマットライセンス710から処理フォーマットライセンス510にフォーマット変換可能であり同様な効果が得られる。

【0083】

尚、伝送フォーマットライセンス変換部および処理フォーマットライセンス判定部は、ライセンスフォーマットの変更などに対応する場合には、ライセンス管理サーバ100およびライセンス中継サーバ110などからのダウンロード、または、物理的なモジュールの置き換えによりアップデートする。

フォーマット変換後は、ライセンス管理サーバ100が生成したライセンスIDでライセンスを管理できるため、伝送フォーマットAライセンスのlicenseID722が処理フォーマットライセンス510のライセンスIDと異なる場合でも、ライセンス管理サーバ100が端末装置120のライセンスを統一的に管理できる。

【0084】

(ライセンス判定S250)

処理フォーマット α ライセンス判定部440は、受信した処理フォーマットライセンス510を、処理フォーマット署名512で検証(ステップS251)する。

尚、本発明は、特定の署名検証方法に依存しないため、少なくとも、署名検証に用いる

公開鍵証明書およびCRL (Certificate Revocation List) が取得できれば、どのような署名検証方法を用いても同様な効果が得られる。

【0085】

改ざんが検出されるなど、署名検証に失敗した場合には、コンテンツ利用を中止する。改ざんされていないことが確認されると処理フォーマットαライセンス判定部440は、処理フォーマットライセンス510から2003年8月31日12時34分56秒まで、最大9回利用可能であることを把握し、例えば、現在時刻が2003年8月1日12時34分56秒で、初回利用であるため、利用可能であると判定(ステップS252)し、コンテンツ処理部450にコンテンツ鍵とコンテンツ処理部でのコンテンツ利用を規定する利用条件を送信する。

利用不可と判定した場合は、コンテンツ利用を中止(ステップS400)する。

(コンテンツ利用S260)

コンテンツ処理部450は、コンテンツ鍵で暗号化コンテンツ810を復号し、利用条件に基づいてコンテンツ利用を制御する。

【産業上の利用可能性】**【0086】**

本発明にかかるコンテンツ配信システム1は、変換フォーマット指定情報711を有し、端末装置120での処理に用いるフォーマットと異なるフォーマットで配信されたライセンスも、端末装置120のフォーマット変換手段が、ライセンスに含まれる変換フォーマット指定情報711により指定されるフォーマットのライセンスに変換するため、ライセンス発行者による端末装置120におけるライセンスの処理フォーマットの指定と、端末装置における受信後のライセンス処理の共通化が可能なコンテンツ配信システムとして有用である。

【0087】

また、本発明にかかるコンテンツ配信システム1は、処理フォーマット署名712を有し、端末装置120での処理に用いるフォーマットと異なるフォーマットで配信されたライセンスを処理に用いるフォーマットに変換した後にデジタル署名によるライセンスの改ざん検出が可能なコンテンツ配信システムとして有用である。

さらに、本発明にかかるコンテンツ配信システム1は、フォーマット変換後もライセンス管理サーバ100が生成したライセンスIDと同じライセンスIDを用いることにより、異なるフォーマットで配信されたライセンスでもライセンス管理サーバ100が端末装置120のライセンスを統一的に管理することが可能なコンテンツ配信システムとして有用である。

【図面の簡単な説明】**【0088】**

【図1】本発明の実施の形態に係るコンテンツ配信システム1の全体の概略構成を示す図である。

【図2】本発明の実施の形態におけるライセンス管理サーバ100の構成を示す図である。

【図3】本発明の実施の形態におけるライセンス中継サーバ110の構成を示す図である。

【図4】本発明の実施の形態における端末装置120の耐タンパ部410の構成を示す図である。

【図5】処理フォーマットライセンス510の記述例である。

【図6】XML言語によるライセンス本体511と処理フォーマット署名512の記述例である。

【図7】伝送フォーマットライセンス710の記述例である。

【図8】暗号化コンテンツ810の構造図である。

【図9】コンテンツ配信システム1におけるライセンスの作成までの処理概略を示すフロー図である。

【図10】コンテンツ配信システム1における暗号化コンテンツとライセンスの配信からコンテンツ利用までの処理概略を示すフロー図である。

【図11】ライセンス管理サーバ100の処理を示すフロー図である。

【図12】ライセンス中継サーバ110の処理を示すフロー図である。

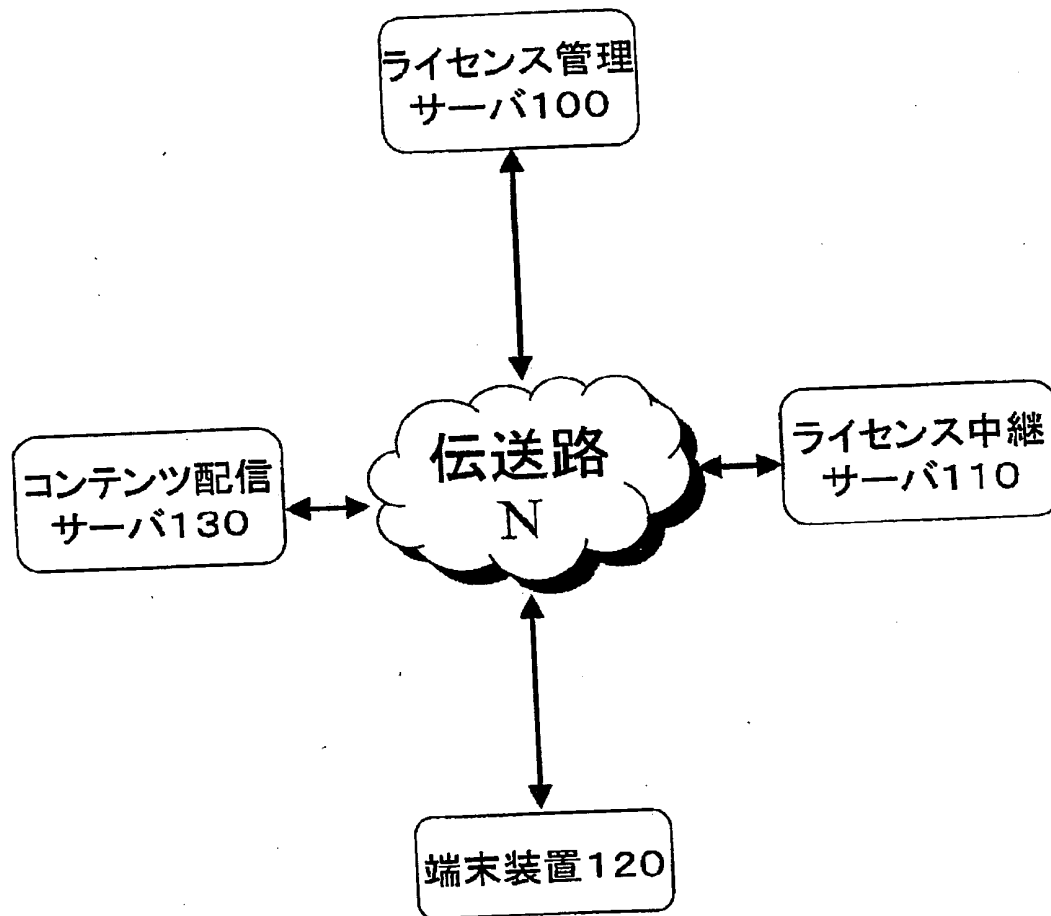
【図13】端末装置120の処理を示すフロー図である。

【符号の説明】

【0089】

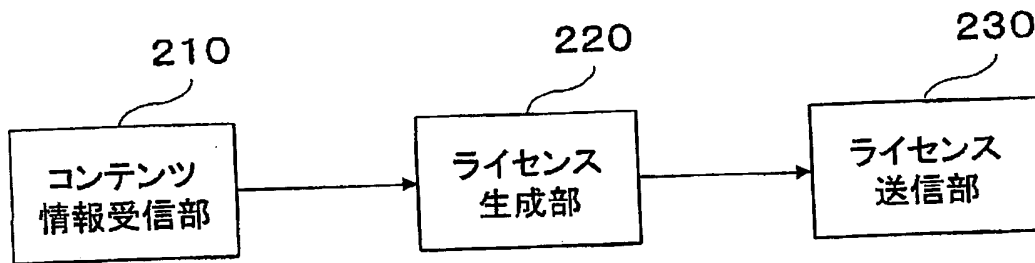
- 1 コンテンツ配信システム
- 100 ライセンス管理サーバ
- 110 ライセンス中継サーバ
- 120 端末装置
- 130 コンテンツ配信サーバ
- 210 コンテンツ情報受信部
- 220 ライセンス生成部
- 230 ライセンス送信部
- 310 ライセンス生成情報受信部
- 320 ライセンス変換部
- 330 ライセンス送信部
- 410 耐タンパ部
- 420 第1のライセンス処理部
- 421 第2のライセンス処理部
- 430 伝送フォーマットAライセンス変換部
- 431 伝送フォーマットBライセンス変換部
- 440 処理フォーマット α ライセンス処理部
- 441 処理フォーマット β ライセンス処理部
- 450 コンテンツ処理部

【書類名】図面
【図 1】

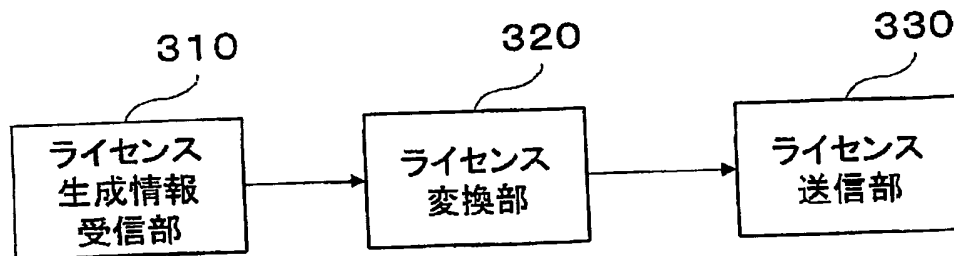


コンテンツ配信システム1

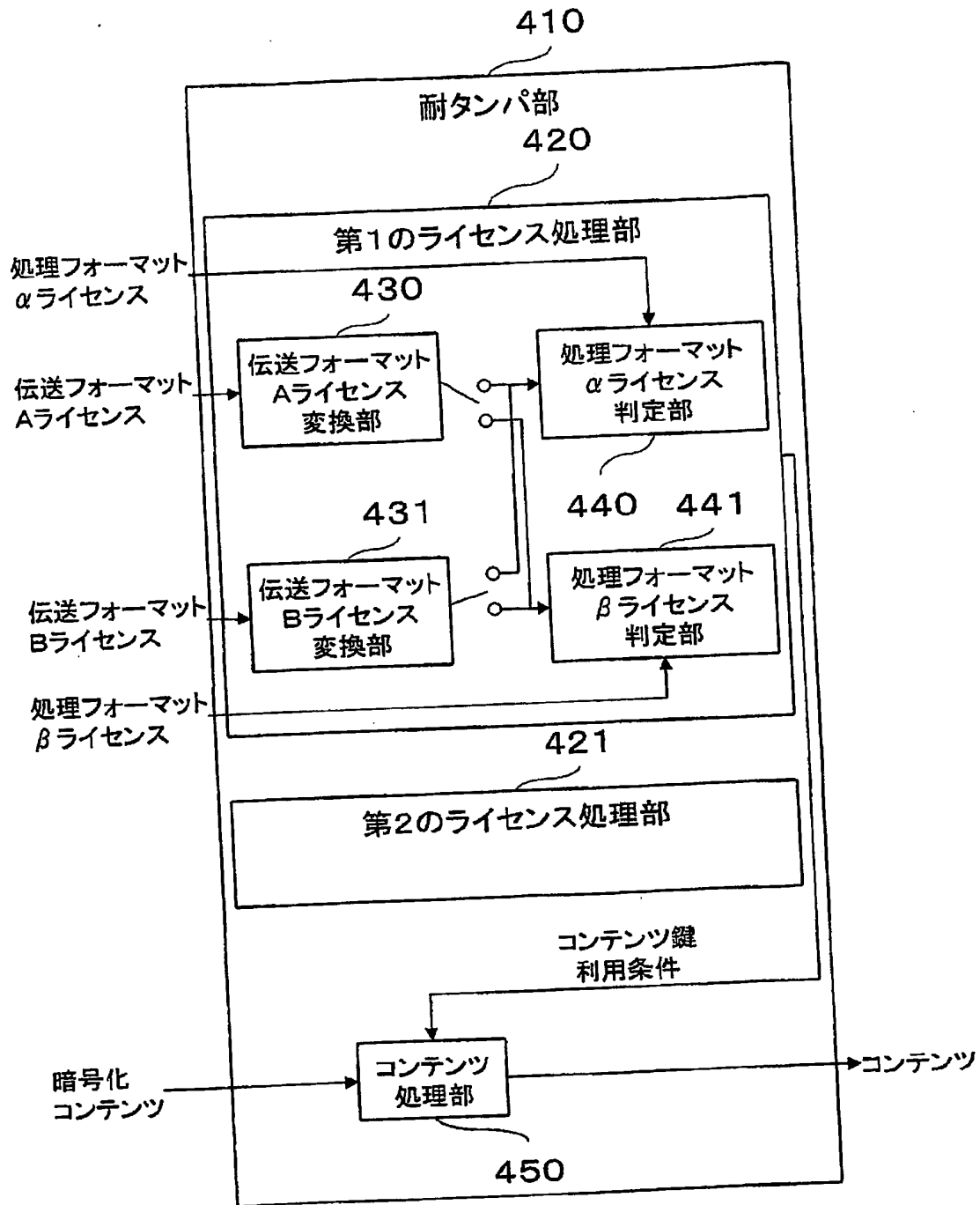
【図 2】



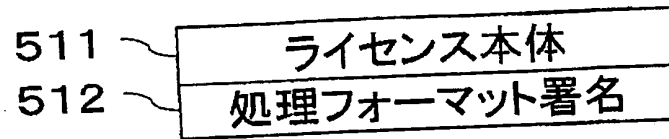
【図 3】



【図 4】



【図 5】



処理フォーマットライセンス 510

【図 6】

```
<license>
  <grantGroup>
    <grantGroup>
      <GrantGroup>
        <grant>
          <Grant>
            <right><play_main/></right>
            <resource>
              <resourceContent>
                <contentID>02</contentID>
                <contentKey>0001</contentKey>
              </resourceContent>
            </resource>
            <allConditions>
              <condition>
                <exerciseLimit>
                  <maxCount>9</maxCount>
                </exerciseLimit>
              </condition>
            </allConditions>
          </Grant>
        </grant>
      </GrantGroup>
    </grantGroup>
  </grantGroup>
  <licenseGeneralInformation>
    <drmID>0001</drmID>
    <version>0100</version>
    <licenseID>02</licenseID>
    <licenseValidityTimePeriod>
      <endTimePoint>20030831123456Z</endTimePoint>
    </licenseValidityTimePeriod>
  </licenseGeneralInformation>
</license>

<signature>0123456789....0123456789</signature>
```

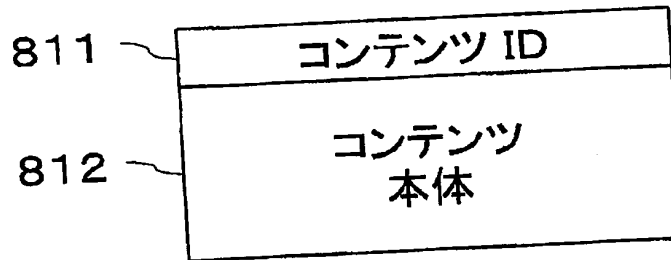
【図 7】

711	変換フォーマット指定情報
712	処理フォーマット署名
713	関連情報長
714	記述子タグ
715	記述子長
716	drmID
717	記述子タグ
718	記述子長
719	version
720	記述子タグ
721	記述子長
722	licenseID
723	記述子タグ
724	記述子長
725	right
726	記述子タグ
727	記述子長
728	maxCount
729	記述子タグ
730	記述子長
731	contentID
732	記述子タグ
733	記述子長
734	contentKey
735	記述子タグ
736	記述子長
737	endTimePoint
760	改ざん検出

ライセンス
本体750

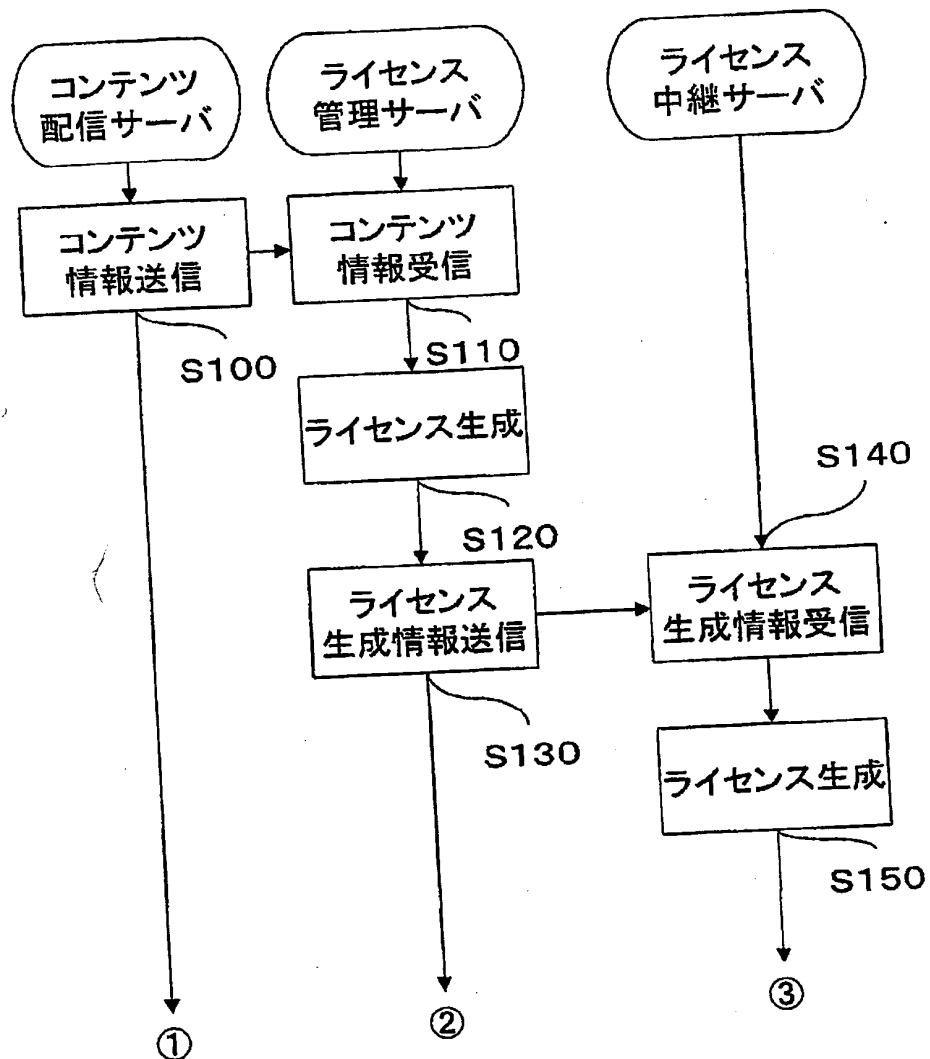
伝送フォーマットライセンス 710

【図 8】

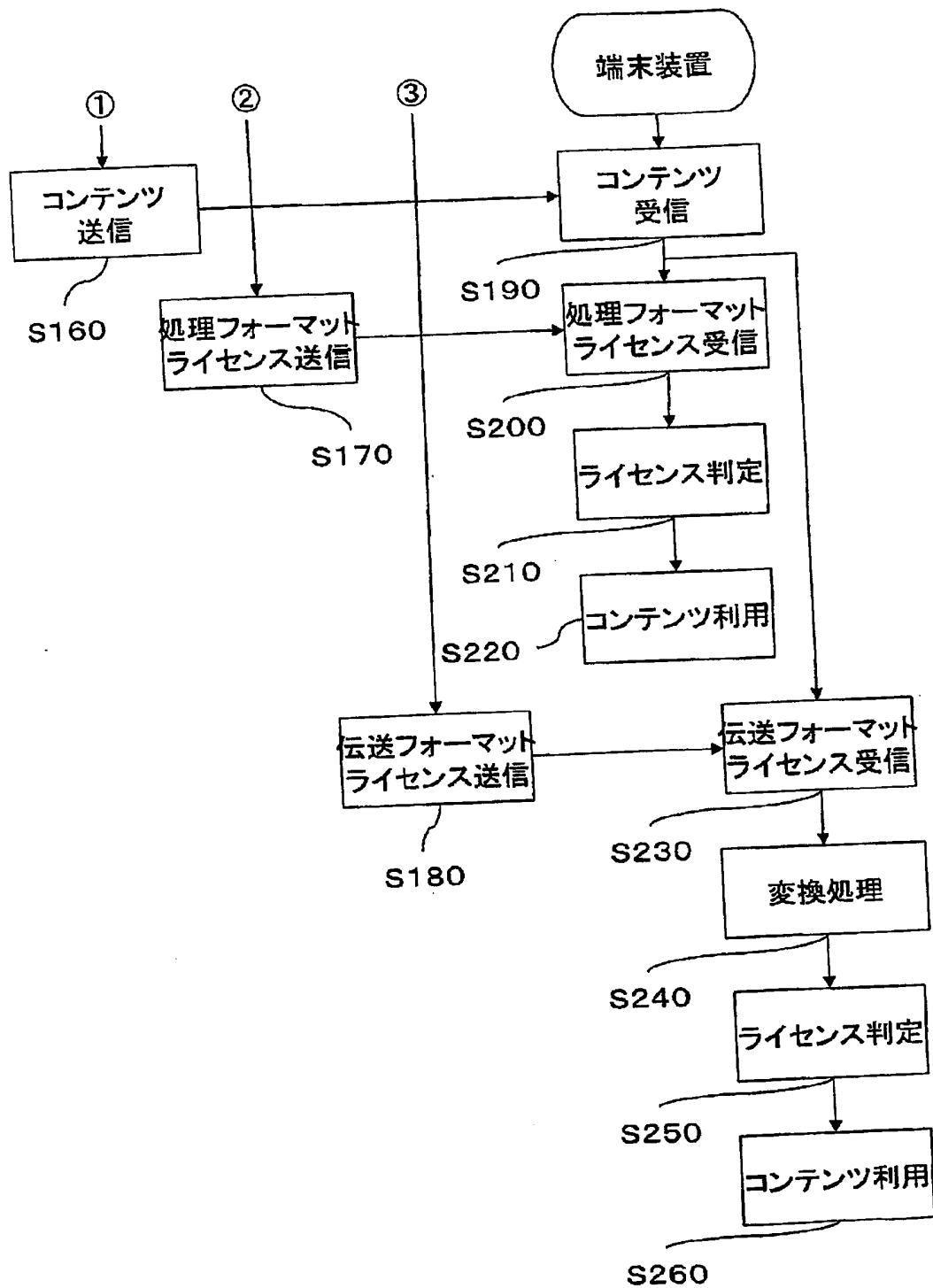


暗号化コンテンツ 810

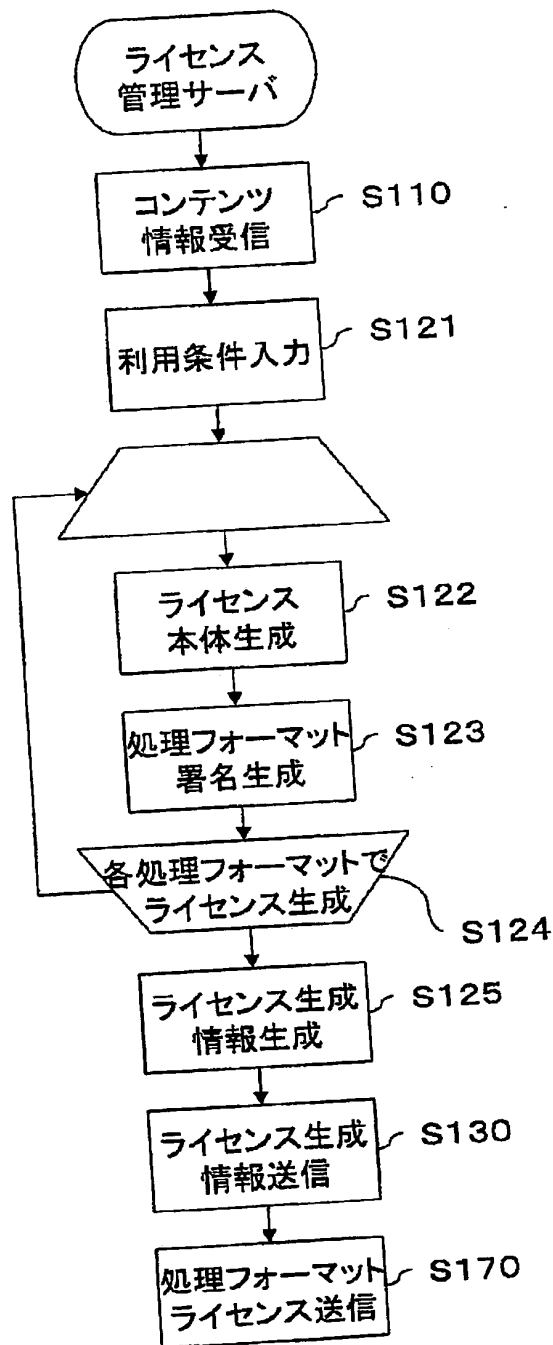
【図 9】



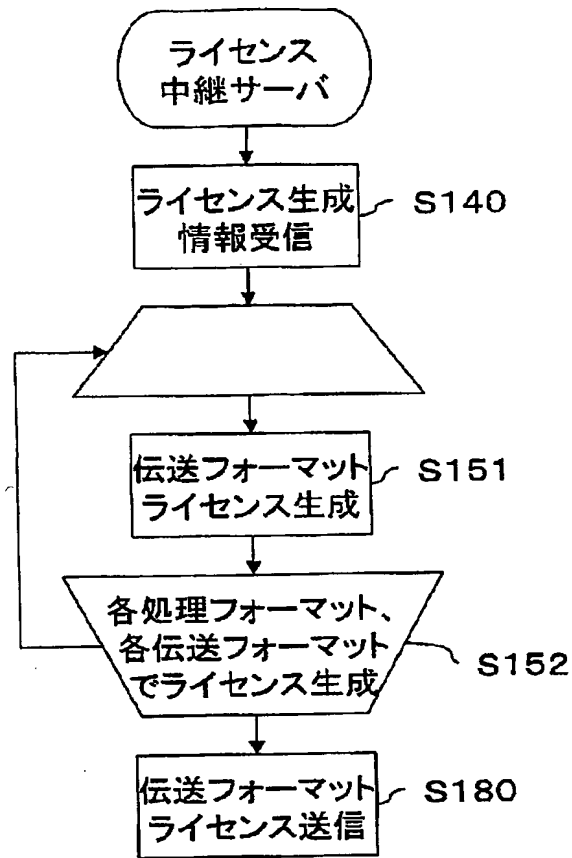
【図10】



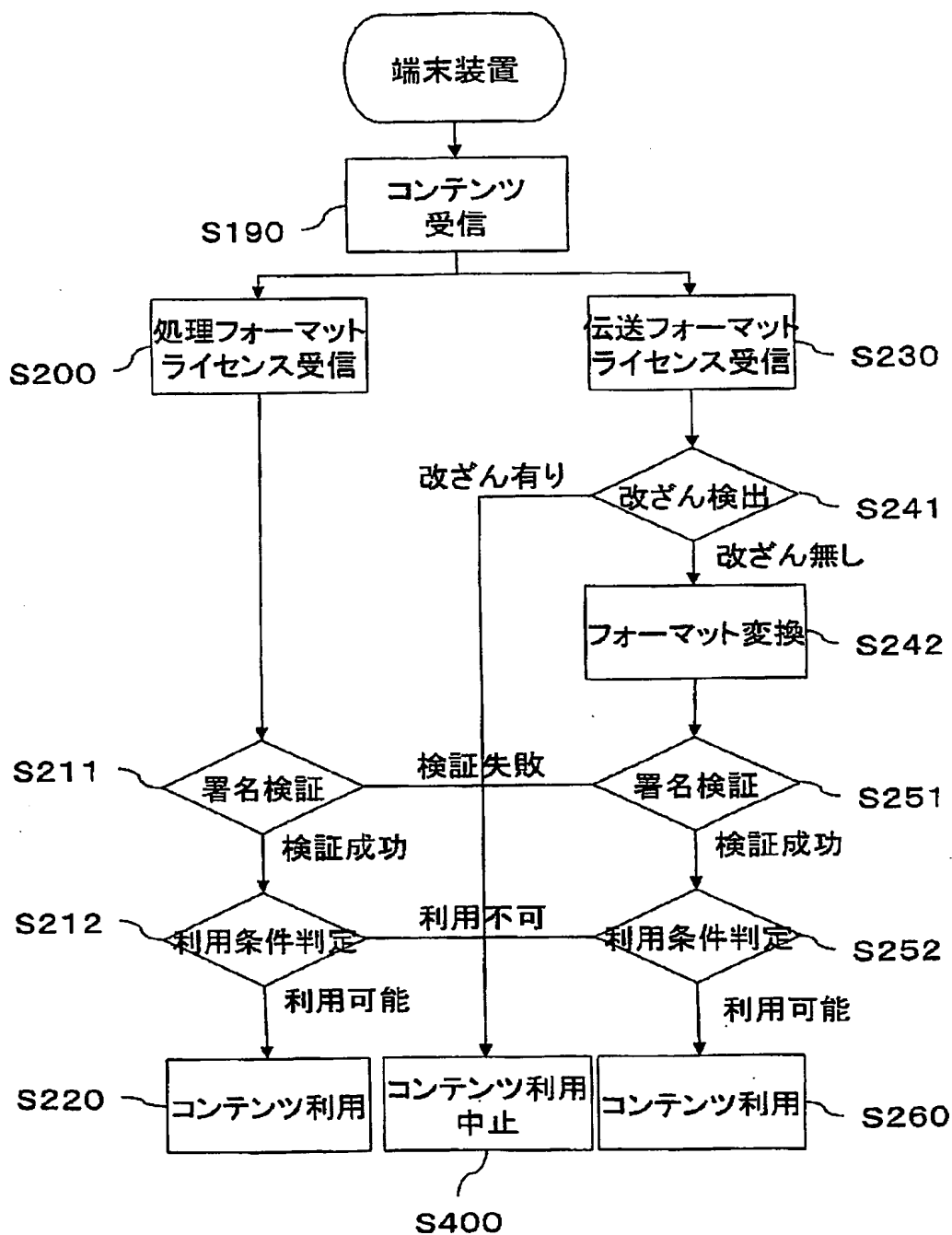
【図 11】



【図 12】



【図13】



【書類名】 要約書

【要約】

【課題】 端末装置で受信したライセンスのフォーマットを変換する場合でも、ライセンス発行者の指定したフォーマットに変換し、フォーマット変換後のライセンスの改ざん検出が可能なコンテンツ配信システムを提供する。

【解決手段】 伝送フォーマット A ライセンス変換部 430 が、ライセンス変換部伝送フォーマットライセンス 710 を変換フォーマット指定情報 711 で指定される処理フォーマットライセンス 510 に変換し、処理フォーマット署名 712 で署名検証することで改ざん検出する。

【選択図】 図 4

認定・付加情報

特許出願の番号	特願 2004-003431
受付番号	50400027992
書類名	特許願
担当官	第七担当上席 0096
作成日	平成16年 1月 9日

<認定情報・付加情報>

【提出日】 平成16年 1月 8日

特願 2 0 0 4 - 0 0 3 4 3 1

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日
[変更理由]
住 所
氏 名

1 9 9 0 年 8 月 2 8 日
新規登録
大阪府門真市大字門真 1 0 0 6 番地
松下電器産業株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/019287

International filing date: 16 December 2004 (16.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-003431
Filing date: 08 January 2004 (08.01.2004)

Date of receipt at the International Bureau: 10 February 2005 (10.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record.**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.